

# Information Technology Security Policy

Adopted by the Information Services Board (ISB) on July 14, 2000

**Policy No: 400-P1**

Also see: [401-S1](#), [402-G1](#)

Supersedes No: N/A

Effective Date: October 6, 2000

Revision Date: April 2002

[Definitions](#)

## Table of Contents

|                          |   |
|--------------------------|---|
| Purpose.....             | 1 |
| Statutory Authority..... | 3 |
| Scope .....              | 3 |
| Exemptions .....         | 3 |
| Policy.....              | 3 |
| Maintenance.....         | 6 |

## Purpose

The purpose of this Information Technology (IT) Security Policy is to create an environment within State of Washington agencies that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. The state's transition from multiple proprietary network connections over dedicated leased networks to the Internet for conducting vital public business has highlighted the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information;
- Misuse - The use of information assets for other than authorized purposes by either internal or external users;
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users;
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs;
- Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization; and

- Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component.

Because information technology security planning is primarily a risk management issue, this policy and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

- Common approaches to end-user authentication;
- Consistent and adequate network, server, and data management;
- Appropriate uses of secure network connections; and
- Closing unauthorized pathways into the network and into the data pursuant to RCW 43.105.017(2).

Such an environment is made possible through an enterprise approach to security in state government that:

- Promotes an enterprise view among separate agencies;
- Requires adherence to a common security architecture and its related procedures;
- Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
- Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.

In response to these threats and to assist state agencies in mitigating associated risks, the Information Services Board (ISB) requires that agencies take steps necessary to initiate an enterprise-wide approach to:

- Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment;
- Ensure secure interactions between and among business partners, external parties and state agencies utilize a common authentication process, security architecture, and point of entry;
- Prevent misuse of, damage to, or loss of IT hardware and software facilities;
- Ensure employee accountability for protection of IT assets; and
- Prevent unauthorized use or reproduction of copyrighted material by public entities.

Accordingly, the ISB directs state agencies to:

- Operate in a manner consistent with the Information Technology (IT) Security Policy of the State of Washington;
- Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and computer data computing and telecommunications facilities -- including telephones, hardware, software, and personnel -- against security breaches;

- Train staff to follow security procedures and standards;
- Apply appropriate security measures when developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce); and
- Ensure and oversee compliance with this policy.

### **Statutory Authority**

The provisions of RCW 43.105.041 detail the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards and procedures.

### **Scope**

This policy applies to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage or use IT services or equipment to support critical state business functions.

For the purposes of this policy, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by an agency and to protect IT assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of IT facilities and off-site data storage; computing, telecommunications, and applications related services purchased from other state agencies or commercial concerns; and Internet-related applications and connectivity.

### **Exemptions**

This policy applies to Institutions of Higher Education, except, pursuant to RCW 43.105.200, when they develop security policies in lieu of the policy statements below that are: a) appropriate to their respective environments, and b) consistent with the intent of the Information Services Board. Such higher education security policies must address:

- Appropriate levels of security and integrity for data exchange and business transactions;
- Effective authentication processes, security architecture(s), and trust fabric(s); and
- Compliance, testing and audit provisions.

### **Policy**

It is the IT security policy of the state of Washington that:

1. Each agency shall operate in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of sensitive data and business transactions. Agencies may establish certain autonomous applications, including those hosted by an Applications Service Provider or other third party, outside of the shared, trusted environment, PROVIDED the establishment and

operation of such applications does not jeopardize the enterprise security environment, specifically:

- The security protocols (including means of authentication and authorization) relied upon by others; and,
  - The integrity, reliability, and predictability of the state backbone network.
2. Each agency shall establish its secure state business applications within the Washington State Digital Government framework. This requires that all parties interact with agencies through a common security architecture and authentication process. DIS shall maintain and operate the shared infrastructure necessary to support applications and data within a trusted environment.
  3. Furthermore, each agency that operates its applications and networks within the Washington State Digital Government framework must subscribe to the following principles of shared security:
    - Agencies shall follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;
    - Agencies shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;
    - Agencies shall follow security standards established for securing servers and data associated with the secure application; and
    - Agencies shall follow security standards established for creating secure sessions for application access.
  4. Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses. Plans for Internet-based transactional applications, including but not limited to e-commerce, must be prepared and incorporated into the agency's portfolio and submitted for security validation.\*
  5. Each agency must ensure staff is appropriately trained in IT security procedures. Each agency must make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible. Agencies are encouraged to participate in appropriate security alert response organizations at the state and regional levels.
    - All Internet applications should be included and managed within the agency portfolio. As required by the IT Security Standards, a detailed security design packet for transactional, non-anonymous applications (including but not limited to those using a security mechanism for access control) is submitted for review by DIS but the security related information need not be included in the portfolio.

Examples of security mechanism for access control include, but are not limited to, Public Key Infrastructure, User ID and passwords, or biometrics.

6. Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.
7. Each agency must conduct an IT Security Policy and Standards Compliance Audit once every three years. The audit must be performed by knowledgeable parties independent of the agency's IT organization, such as the State Auditor. The work shall follow audit standards developed and published by the State Auditor. The State Auditor may determine an earlier audit of an agency's IT processing is warranted, in which case they will proceed under their existing authority. The nature and scope of the audit must be commensurate with the extent of the agency's dependence on secure IT to accomplish its critical business functions. Each agency must maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit. To the extent that the audit documentation includes valuable formulae, designs, drawings, computer source codes, object codes or research data, or that disclosure of the audit documentation would be contrary to the public interest and would irreparably damage vital government functions, such audit documentation is exempt from public disclosure. See RCW 42.17.310 and 42.17.330.
8. Pursuant to RCW 43.105.017(3), agency heads are responsible for the oversight of their respective agency's IT security and will confirm in writing that the agency is in compliance with this policy. The annual security verification letter must be included in the agency IT portfolio and submitted to the Board. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as updates to them since the last approval. The head of each agency must provide annual certification to the ISB by August 31 of each year that an IT Security Program has been developed, implemented, and tested.
9. The State Auditor may audit agency IT security processes, procedures, and practices. The State Auditor may audit any agency pursuant to RCW 43.88.160 for agency compliance with this policy.

Agency IT security processes, procedures, and practices may contain information (confidential or private) about the agency's business, communications, and computing operations or employees. Policy and procedures for distribution of any related

documentation should consider sensitive information and related statutory exemptions for such information from public disclosure. See RCW 42.17.310 and 42.17.330.

### **Maintenance**

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.